IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

JOHN DOE, on behalf of themselves and all others similarly situated Plaintiff v. PROMEDICA HEALTH SYSTEMS, INC. Defendant	CASE NO. 3:20-CV-01581 JUDGE JACK ZOUHARY

PLAINTIFF'S MEMORANDUM IN SUPPORT OF MOTION TO REMAND

This case arises out of Defendant's disclosures of personally identifiable patient data and communications to Facebook, Google, Microsoft, and Quantcast. Compl. at ⁋⁋ 5-10. ProMedica disclosed this information without plaintiff's knowledge or consent through its deployment of invisible web bugs at its properties that identified when patients logged in to the ProMedica patient portal and disclosed those patients' communications with ProMedica, their healthcare provider, about providers, conditions, treatments, and more. *Id.*

Plaintiff filed the underlying action in Ohio state court alleging Ohio common law causes of action for (1) unauthorized disclosure of non-public medical information pursuant to *Biddle v. Warren General Hospital*, 86 Ohio St. 3d 395 (1995); (2) breach of confidence; and (3) invasion of privacy. Plaintiff, an Ohio citizen, filed a lawsuit alleging Ohio claims against his Ohio healthcare provider involving care and communications that took place in Ohio. Nevertheless, Defendant filed a Notice of Removal on July 17, 2020, ECF No. 1, claiming federal officer removal under 28 U.S.C. § 1442(a)(1) despite lacking a government contract or any other federal delegation of authority justifying removal. For the reasons stated herein, remand is required.

The Promoting Interoperability Program

Defendant fails to identify any federal directive, duty, or control over its web properties or patient portal. Nor does it identify any federal directive, duty, or control of the activities at the heart of this case: routine disclosures of patient personally identifiable data and communications to third-party marketing companies without authorization. Instead, Defendant relies on the federal government's general interest in improving health information technology through what is known as the "Promoting Interoperability" Program, which Defendant incorrectly refers to as the "Meaningful Use" Program. But Defendant's omissions are telling.

First, unlike the cases Defendant relies on, it is undisputed that Defendant does not have a contract with the federal government relevant to the allegations in this case.

Second, the Promoting Interoperability Program is not required for any hospital or medical provider; it is voluntary. In fact, participation in the program does not even require providers to maintain a website or patient portal. *See* CMS, *EHR Incentive Program Stage 3 Rule*, 80 FR 62842 (Oct. 16, 2015). And even if a hospital creates an online patient portal (despite no obligation to do so), it is not even required to show that a single patient actually used an online patient portal in order to qualify for incentives. *See* 42 C.F.R. § 495.24(e).

Third, the Promoting Interoperability Program does not involve any federal supervision. Rather, a hospital that participates in the program need only "attest" that it used "certified EHR" and specify the technology. 42 C.F.R. § 495.40(b)(2)(i).

Fourth, the Promoting Interoperability Program does not direct, authorize, or guide hospitals or other providers to deploy third-party marketing tools that cause the disclosures of patients' personally identifiable data to companies like Facebook anywhere on their web properties, much less their patient portals.

Fifth, rather than impose a duty on hospitals to share patient data with Facebook in connection with the creation and maintenance of patient portals, the federal authorities Defendant cites consistently impose the opposite duty. For example, from its start, ONC has had a duty to "ensure[] that patients' individually identifiable health information is secure and protected." E.O. 13335 § 2(f) at 703. The HITECH Act, which Defendant cites as a source for a purported duty to disclose patient information to Facebook and others actually strengthened federal prohibitions on the sale of patient data and the use of patient data for marketing purposes in the absence of specific, informed, written patient authorization. *See* HITECH Act, §§ 1304-06. In truth, Defendant's disclosures are not lawful. Indeed, under HIPAA, the sale of a patient list to a marketing firm" is not permitted, and "a covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which would include disclosure of patient status. *See* 65 FR 82717 (Dec. 28, 2000); 67 FR 53186 (Aug. 14, 2002). Moreover, HIPAA would not preempt state law, as "[n]o requirement of meaningful use supersedes any Federal, State, or local law regarding the privacy of a person's health information." CMS, *Meaningful Use State 2 Final Rulemaking*, 77 FR 54008 (Sept. 4, 2012). Finally, CMS has consistently explained that "[p]rotecting electronic health information is essential to all other aspects of meaningful use" because "[u]nintended and/or unlawful disclosures of personal health information could diminish consumers' confidence in EHRs and electronic health information exchange." *Stage 2 Final Rule*, 77 FR 54002 (Sept. 4, 2012); *Promoting Interoperability Final Rule*, 83 FR 41640 (Aug. 17, 2018).

I. LEGAL STANDARD FOR FEDERAL OFFICER REMOVAL

The federal officer removal statute provides that a civil action may be removed to federal court where the action is "against or directed to … [t]he United States or any agency thereof or

any officer (or any person acting under that officer) of the United States or of any agency thereof, in an official or individual capacity, for or relating to any act under color of such office[.]" 28 U.S.C. § 1442(a)(1). A party seeking removal "bear[s] the burden of establishing federal court jurisdiction" and must prove: (1) the defendant is a "person" within the meaning of the statute; (2) the defendant "acted under a federal officer;" (3) the defendant's actions in question were "performed under color of federal office;" and (4) that the defendant "raise[s] a colorable federal defense." *Mays v. City of Flint*, 871 F.3d 437, 442-43 (6th Cir. 2017). In addition, "removal statutes are to be strictly construed, and all doubts should be resolved against removal." *Id*.

While Defendant is a "person," it fails the other three elements of the *Mays* test.

A. ProMedica is Not *Acting Under* a Federal Officer in Any Respect, Much Less When It Discloses Patient Personally Identifiable Data and Communications to Facebook and Others for Marketing Purposes

"[T]he fact that a regulatory agency directs, supervises, and monitors a company's activities in considerable detail" does not make the company one *acting under* a federal officer. *Watson v. Phillip Morris Cos., Inc*., 551 U.S. 142, 145 (2007). Instead, for a private company, acting under refers to "a relationship that involves 'acting in a certain capacity, considered in relation to one holding a superior position or office." *Id*. at 151-52. An "acting under" relationship "typically involves subjection, guidance, or control" and "must involve an effort to assist, or to help carry out, the duties or tasks of the federal superior." *Id*. (internal citation omitted). Thus, federal officer removal is improper when there is "no evidence of any delegation of legal authority" nor "evidence of any contract, any payment, any employer/employee relationship, or any principal/agent arrangement." *Id*. at 156.

Without a contract, there is no government contractor removal. A recent court held that "[w]ithout a contract, the government has not validly conferred any authority on a private company

to carry out a project on its behalf or otherwise gets its work done." *In re: 3M Combat Arms Earplug Products Liab. Litig*., 2020 WL 4275646 (N.D. Fl. Jul. 24, 2020) (quotation omitted).

In *Mays*, the most analogous Sixth Circuit case, the Michigan Department of Environmental Quality (MDEQ) sought removal based on its relationship with the EPA, from whom it received funding and jointly enforced environmental laws. The Sixth Circuit remanded the case, holding "that the defendant seeking removal must be in a relationship with the federal government where the government is functioning as the defendant's superior." 871 F.3d at 444.

The *Mays* defendants argued that receipt of federal funds to enforce federal law justified removal. The Sixth Circuit disagreed, holding that, "receipt of federal funding alone cannot establish a delegation of legal authority[.]" *Id*. The court explained that "a government contractor entitled to removal would presumably be contractually required to follow the federal government specifications in making products or providing services" and "would not ordinarily have any authority to take actions beyond those specified in the contract." *Id*. at 445.

The *Mays* defendants argued that government contractor removal did not require an actual government contract, but the Sixth Circuit found that every case the defendants relied upon involved a contractual agreement of some sort. Therefore, it held "that the absence of language allowing a private entity to act on the federal government's behalf weighs against allowing federal-officer removal." *Id*. at 445 (*citing Ohio State Chiropractic Ass'n v. Human Health Plan, Inc*., 647 F. App'x. 619, 623-24 (6th Cir. 2016) (explaining that a Medicare Advantage Organization could *not* invoke the federal officer removal statute because the relevant regulations did not permit the organization to act on the government's behalf; the organization had the freedom to use some innovative private market techniques; the government was not controlling the entity's daily

operations; and the government would not have to perform the exact same tasks in the absence of a contractual arrangement)).

Here, Defendant fares no better. It fails to allege that the government was even aware of its website and portal much less facts showing "any delegation of legal authority," "any contract," "any employer/employee relationship, or any principal/agent arrangement." Quite simply, the federal government exercised zero direct control over Defendant regarding its development, design, and implementation of its web properties and portal.

In the absence of any factual support substantiating it was acting under a federal office, Defendant's notice merely regurgitates the *Bennett* factors for government contractor removal. *See* ECF No. 1. at ¶¶ 25-30 (citing *Bennett v. MIS Corp*., 607 F.3d 1076 (6th Cir. 2010)). In *Bennett*, the Sixth Circuit found removal appropriate for a government contractor hired to remediate mold and other environmental hazards at government-owned properties. In support of removal in that case, the defendant "attached its FAA contracts … [which] included precise specifications" and required federal officers to closely monitor the defendant's work. *Id*. at 1087. "Specifically, each contract designated a federal officer who 'directly' supervised each remediation" and "were prohibited from modifying or deviating from the FAA's specifications without first obtaining 'the signature of the Lead Contractor Officer,' Judy Ryckman, also an FAA officer." *Id*. The supervising federal officers also had the authority to "require" the defendant to fire employees, controlled the working hours of defendant's employees, and prohibited defendant's employees from being on the worksite without an FAA escort and/or prior approval. *Id*.

Here, Defendant's government contractor argument fails for the simple fact that it is not a government contractor. And even if Defendant could assert that the voluntary provisions of the

Promoting Interoperability Program constituted a "quasi-contract," those provisions are not exacting enough to create the principal/agent relationship necessary for federal officer removal.

First, when ProMedica argues that it is "helping the government produce the nationwide, interoperable information technology infrastructure for health information" it fails to cite any facts supporting its bare allegation that the federal government is or would be "producing patient portals." Moreover, Defendant's argument ignores the primary purpose and goals of the voluntary Promoting Interoperability Program—to maintain patient privacy—and the fact that the underlying case is not at all relevant to that program. ECF No. 1 at ¶ 27.

In *Ohio State Chiropractic*, the Court asked whether Medicare Advantage organizations "perform a job that the government would have to perform itself if it did not contract with private firms?" "We think not," the Court answered. "If no health insurer chose to contract with CMS as an MAO, it is doubtful that the government would get into the business of offering its own MA plans. It certainly doesn't have to." 647 F. App'x. at 624. The same question should be asked here: in fashioning a patient portal for its own patients (including non-Medicaid and non-Medicare patients), has Defendant alleged any plausible set of facts that it was performing a job that the government would have to perform for itself in the absence of a relationship with private firms? The answer is the same as *Ohio State Chiropractic*: no. The federal government has not nationalized the collection and maintenance of electronic health records. Thus, it would not create its own federally operated patient portal to house medical records for ProMedica patients.

Second, when Defendant argues that, "in the absence of ProMedica's actions (and the work of comparable medical providers throughout the country), the federal government would be left alone to complete its mission," it ignores that the federal government's mission regarding electronic health records. ECF No. 1 at ¶ 28. As the program's very name implies, Promoting

Interoperability's mission is to promote the interoperability of patient health records, *i.e.*, to ensure that providers use electronic records in a way that is interoperable amongst providers.

Third, Defendant claims without alleging any facts that "the government has specified how to best enhance patient engagement, including through a patient portal" and "has clarified how to design the portals, and has told entities how best to market their on-line resources." (Doc. 1 at ¶ 29). Yet, Defendant has not alleged any facts supporting the notion that the government has ever required, encouraged, or condoned the use of any third-party marketing tools surrounding a patient portal.

Even if Defendant could produce evidence it claims is instructive, the Sixth Circuit has rejected such arguments when, as here, the federal entity "was not involved in the key action underlying the Plaintiffs' complaint" and Defendant's "notice of removal [did] not identify any specific actions or inactions alleged in the complaint that the [federal entity] required [defendants] to take or refrain from taking." *Mays*, 871 F.3d at 446. Similarly, here, Defendant has failed to identify any federal officer involvement in its decision to deploy source code that caused disclosures of patient data to be made to Facebook from its properties. To the contrary, Plaintiff has submitted an expert Declaration that Defendant removed much of the offending source code from its property after Plaintiff filed suit. Smith Decl. ¶ 4. This begs the question: if the federal officer required Defendant to place the source code on its property as Defendant asserts, how then could the Defendant remove the source code on its own soon after the Plaintiff filed suit?

Fourth, Defendant's unsupported claim that the government has "closely monitored the work of private entities (like ProMedica), ECF No. 1 at ⁋ 30, is false. In *Bennett*, the Sixth Circuit explained the types of facts necessary to justify federal officer removal. In that case, the private company asserting federal officer status provided the court with an actual contract that included

precise specifications on how it was to perform the work; assigned specific federal officers to closely monitor the work; prohibited any modification without specific approval; granted the overseeing federal officers the authority to require dismissal of employees; determined exactly when the company worked on the project; and required the company's employees to be escorted by FAA employees at all times. *Bennett*, 607 F.3d at 1087-88.

In this case, not a single one of these qualities exist. Instead, Defendant must only "attest" that it is using certified electronic health record technology to qualify for the voluntary program. This is not enough. *See Mays*, 871 F.3d at 446 (holding that "compliance reporting, even if detailed, is insufficient by itself to merit federal officer removal."); *see also Panther Brands, LLC v. Indy Racing League, LLC*, 827 F.3d 586, 590 (7th Cir. 2016) ("merely being subject to federal regulations or performing some functions that the government agency controls is not enough to transform a private entity into a federal officer.") (citation omitted).

Simply because an industry is heavily regulated, it does not follow that the regulated entities are acting under a federal officer. Airplane manufacturing provides one such example. *See Lu Junhong v. Boeing Co.*, 792 F3d 805, 809 (7th Cir. 2015) (holding that "being regulated, even when a federal agency directs, supervises, and monitors a company's activities in considerable detail is not enough to make a private firm a person acting under a federal agency." (quotation omitted)); *see also Riggs v Airbus Helicopters, Inc.*, 939 F.3d 981, 990 (9th Cir. 2019) (holding that "an aircraft manufacturer does not act under a federal officer when it exercises designated authority to certify compliance with governing federal regulations.").

Defendant will likely rely on a recent Western District of Pennsylvania decision, *Doe v. UPMC*, No. 20-cv-359, 2020 WL 4381675 (W.D.Penn. Jul. 31, 2020)[1], but *UPMC* conflicts with

[1] Plaintiffs in that case have moved for certification of the Court's order pursuant to 28 U.S.C. § 1292(b).

binding Sixth Circuit precedent in several ways. *First, UPMC* ruled that the federal officer statute is to be construed "in favor of removal." *Id*. at. *5. This conflicts with *Mays*, which held that "removal statutes are to be strictly construed, and all doubts should be resolved against removal." *Id*. *Second, UPMC* ruled that a party seeking federal officer removal need not establish an agent-principal arrangement or something similar but turns only on whether there is "an effort to assist, or to help carry out, the duties or tasks of the federal superior." *Id*. at*3 (quotation omitted). This conflicts with *Mays'* holding that federal officer removal requires some proof of a "contract or other delegation of legal authority[.]" 871 F.3d at 445. *Third, UPMC* held that "any dispute about whether the allegedly wrongful conduct was outside the scope of the private entity's duties is the very thing that should be left to a federal court to decide." 2020 WL 4381675, at *4. This, too, conflicts with *Mays*, which explains that "a government contractor would not ordinarily have any authority to take actions beyond those specified in the contract." 871 F.3d at 445. *Finally*, the *UPMC* Court accepted false assertions by the defendant about certain duties and responsibilities under federal law.

B. Defendant's Disclosures to Facebook, Google, and Others Were Not "For or Relating to an Act Under Color of Federal Office"

To satisfy the "under color of federal officer" element, a removing party "must show a nexus, a 'causal connection' between the charged conduct and the asserted official authority. In other words, the removing party must show that it is being used because of acts it performed at the direction of the federal officer." *Bennett*, 607 F.3d at 1088. In *Ohio State Chiropractic*, the Court found that a "private billing dispute" between a Medicare provider and a Medicare Advantage organization was not causally connected with the defendant's relationship with the federal officer in question. The same is true here.

This is a private dispute between patients and their healthcare provider about the provider's disclosure of the patients' personally identifiable data to Facebook, Google, and others. There is no relationship to CMS. Nor were there acts "performed *at the direction* of the federal officer." Defendant alleges no facts that a federal officer directed it to deploy source code that discloses patients' personally identifiable data for marketing purposes.

It is important to put Defendant's actions into context. It is obtaining a valuable marketing benefit from placing third-party tracking tools, like the Facebook Pixel, on its property. Compl. at ⁋ 219. That is the "charged conduct" that *Bennett* instructs the Court to analyze in this case. The federal government has not directed Defendant to deploy third-party tracking tools for Defendant's marketing purposes. These disclosures are for Defendant's own gain. HIPAA does not require a healthcare provider to do this—as explained above, HIPAA does not even allow it. Put aside the technological factor in this case: Defendant's conduct is tantamount to giving pages of a patient's confidential medical information to a third party for the third party to use that data in exchange for marketing of its hospital services. Taking Defendant's argument to its logical conclusion, if it had a contract dispute with an Ohio web developer for failing to pay for the development of its website, Defendant is saying it could remove the action to federal court because of the Interoperability Program. Not true.

C. Defendant Does Not Present a 'Colorable' Federal Defense

The final requirement of federal officer removal is that the defendant present a "colorable federal defense" raised in the case. Here, Defendant asserts two potential defenses: (1) that federal law preempts Plaintiff's claims, ECF No. 1 at ¶ 39; and (2) that "traffic on ProMedica's website is not covered" by HIPAA. Neither of these defenses is colorable.

1. HIPAA Does Not Preempt Ohio Law

HIPAA preemption is floor preemption, it does not apply where "[t]he provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification" under HIPAA. 45 C.F.R. § 160.203(b). As ONC explains, providers "need to be aware of … additional applicable federal, state, and local laws governing the privacy and security of health information" because "[s]tate laws that are more privacy-protective of HIPAA continue to apply."[2] It is absurd for Defendant to suggest that HIPAA preempts private common law and other state law causes of action by patients against medical providers for the unauthorized disclosure of patient data when states have nearly unanimously upheld such claims.[3] "The purpose of Congress is the ultimate touchstone in every preemption case." *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996). And, "all preemption cases, … 'start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.'" *Lohr*, at 585, quoting *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947). Even ignoring the clear language of the ONC, HHS, CMS, and HIPAA itself, to accept Defendant's assertion, the Court would have to believe that Congress intended to preempt state laws equally or more restrictive than HIPAA without ever saying as much. But Congress "does not … hide elephants in mouseholes." *Whitman v. American Trucking Association*, 531 U.S. 457, 468 (2001).

2. HIPAA is Not a Federal Defense Here

Putting aside for a moment that Defendant is misinterpreting HIPAA, HIPAA compliance is not dispositive to any of Plaintiff's claims. *See Sheldon v. Kettering Health Network*, 40 N.E.3d

[2] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf at 10.
[3] *See*, for example, *Doe v. Virginia Mason*, 2020 WL 1983046 (Wash. Super. Feb. 12, 2020); *Byrne v. Avery Center for Obstetrics and Gynecology, P.C.*, 175 A.3d 1 (Conn. 2018).

661, 2015-Ohio-3268 (2d. Dist. 2015) (holding that a *Biddle* claim is still cognizable post-HIPAA and that violation of HIPAA did not create negligence per se under Ohio law).

Even if HIPAA is an element of an underlying state law cause of action, it is not a colorable defense. In *Mays*, the Sixth Circuit held that, "'the presence of a claimed violation of [a federal] statute as an element of a state cause of action is insufficiently 'substantial' to confer federal-question jurisdiction." 871 F.3d at 449, quoting *Merrell Dow Pharm. Inc. v. Thompson*, 478 U.S. 804, 814 (1986). And, "where Congress has not created a private cause of action for violations of a federal statute, there is less likely to be a substantial interest in favor of removal." *Id.*

Patient status is personally identifiable health information, making Defendant's HIPAA defense unworkable. Plaintiff's Complaint alleges that Defendant discloses to Facebook every time that a patient clicks to log in to MyChart, ProMedica's patient portal. *See* Compl. at ¶¶ 158, 193. 45 C.F.R. § 160.103 provides that:

> Individually identifiable health information is information that is a subset of health information …, and: (1) is created or received by a health care provider; (2) relates to the past, present, or future physical or mental health or condition of an individual; *the provision of health care to an individual*; or the past, present, or future payment for the provision of health care to an individual; and (i) *that identifies the individual*; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. (emphasis added).

Likewise, HHS has already defined IP addresses as personally identifiable information. *See* 45 C.F.R. § 164.514(b)(2) (IP address numbers, device identifiers, email, "any other unique identifying, characteristic, or code," and any other data that "could be used alone or in combination with other information to identify an individual who is a subject of the information." In addition to patient status disclosures and IP addresses, Defendant also discloses the specific contents of patient communications regarding medical conditions, treatments, providers, and appointments. *See* Compl. at ¶¶ 130-195. These disclosures include specific information that patients send to

Defendant in "risk assessments" for various health conditions. *See* Compl. at ¶¶ 173-191 (breast cancer); 141-158 (coronary artery disease).

Defendant discloses patient status in the same way that disclosing the phone number of a patient who called a provider and used a digital recording system to indicate they were a patient. This violates HIPAA because it is information that "relates to the provision of health care" that either "identifies the individual" or "with respect to which there is a reasonable basis to believe the information can be used to identify the individual." HHS has repeatedly explained:

- "[T]he sale of a patient list to a marketing firm … would not be permitted under this rule without authorization from the individual." 65 F.R. 82717 (Dec. 28, 2000)
- "[C]overed entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list."[4]
- HIPAA protects identifiable data "listed with … an indication that an individual was treated at a certain clinic."[5]
- It would be a violation of HIPAA "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification number[s]" 78 F.R. 5642 (Jan. 25, 2013) (addressing hypothetical of just patient status and identity).

Accordingly, HIPAA is not a colorable defense.

In support of its argument, Defendant cites *Smith v. Facebook*, 262 F. Supp. 3d 943, 954-55 (N.D. Cal. 2017), *aff'd* 745 F. App'x 8 (9th Cir. 2018) (unreported). But *Smith* is inapposite. In *Smith*, the healthcare defendants were dismissed on personal jurisdiction grounds by the district court and the Ninth Circuit decision pertaining to Facebook hinged on interpretation of a Facebook adhesion contract that is no longer in effect. Contract law is state law, not federal law. Further, at oral argument, the Ninth Circuit noted that plaintiffs' real "beef" was "with the medical providers that ought not be putting this stuff out on Facebook where it can be shared and so obviously they've

[4] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html
[5] *See* https://www.hhs.gov/for-professionals/privacy/special-topics/de-identification/index.html

been dismissed for lack of personal jurisdiction, they can be sued elsewhere presumably, but it strikes that this is, if there's a problem, it isn't with Facebook, it's with the healthcare provider."[6]

In *Smith*, the plaintiff was not a patient of any healthcare defendant, nor were all of the healthcare defendants covered entities under HIPAA. Here, Plaintiff is a patient and ProMedica his healthcare provider. In *Smith*, there were no patient portal disclosures. Here, Defendant discloses personally identifiable data to Facebook when a patient logs into the patient portal.

On appeal, the Ninth Circuit held HIPAA did not apply because "the connection between a person's browsing history and his or her own state of health is too tenuous to support" the claim that HIPAA applies. *Smith* at 9. But there's a distinction here: Defendant discloses that Plaintiff is a patient when he logs in to the patient portal. *Doe v. Virginia Mason*, distinguished *Smith*:

> In *Smith*, the federal district court found the Plaintiffs failed to establish personal jurisdiction over the healthcare defendants, the Plaintiff consented to Facebook tracking (this case involves the allegations of sharing data with more than Facebook and does not hinge on the relationship between the Plaintiff and Facebook), and the allegations in this case are broader than sharing URL information alone. This Court does find that the potential disclosure of a specific patient's logging-in to the private portal, possibly coupled with searches of medical providers and conditions immediately prior to log-in, state a claim to a violation of HCIA.

2020 WL 1983046 (Wash. Super. Feb. 12, 2020). Thus, *Smith* is not relevant. To Plaintiff's knowledge, the only federal court to have considered the issue concluded that patient status alone is protected. *See Arvidson v. Buchar*, 2018 WL 10613032 (V.I. Jun. 6, 2018).

[6] Oral Argument at 6:423, https://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000014448

CONCLUSION

For the foregoing reasons, Plaintiff requests that the Court remand this case to the Lucas County Court of Common Pleas.

Respectfully submitted,

s/ Kevin C. Hulick
STUART E. SCOTT (0064834)
KEVIN C. HULICK (0093921)
SPANGENBERG SHIBLEY & LIBER LLP
1001 Lakeside Avenue East, Suite 1700
Cleveland, OH 44114
(216) 696-3232
(216) 696-3924 (FAX)
sscott@spanglaw.com
khulick@spanglaw.com

MITCHELL BREIT (*pro hac vice*)
JASON 'JAY' BARNES (*pro hac vice*)
SIMMONS HANLY CONROY LLC
112 Madison Avenue, 7th Floor
New York, NY 10016-7416
(212) 784-6400
(212) 213-5949 (FAX)
mbreit@simmonsfirm.com
jaybarnes@simmonsfirm.com

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 17th day of August 2020, I electronically filed the foregoing with the Clerk of Court by using the CM/ECF System. Copies will be served upon counsel of record by, and may be obtained through, the Court CM/ECF Systems.

s/ Kevin C. Hulick
STUART E. SCOTT (0064834)
KEVIN C. HULICK (0093921)
SPANGENBERG SHIBLEY & LIBER LLP
1001 Lakeside Avenue East, Suite 1700
Cleveland, OH 44114
(216) 696-3232
(216) 696-3924 (FAX)
sscott@spanglaw.com
khulick@spanglaw.com

Counsel for Plaintiff and the Proposed Class